To print: Select **File** and then **Print** from your browser's menu

---

This story was printed from ZDNN,
located at http://www.zdnet.com/zdnn.

DVD encryption break is a good thing

By *Bruce Schneier*, Special to ZDNet
November 16, 1999 12:23 PM PT
URL:

The scheme to protect DVDs has been broken. There are now freeware programs on the Net that remove the copy protection on DVDs, allowing them to be played, edited, and copied without restriction.

This should be no surprise to anyone, least of all to the entertainment industry.

The protection scheme is seriously flawed in several ways. Each DVD is encrypted with something called Content Scrambling System (CCS). It has a 40-bit key. (I have no idea why. The NSA and the FBI shouldn't care about DVD encryption. There aren't any encrypted terrorist movies they need to watch.) It's not even a very good algorithm. But even if the encryption were triple-DES, ths scheme would be flawed.

Every DVD player, including hardware consoles that plug into your television and software players that you can download to your computer, has its own unique unlock key. (Actually, each has several. I don't know why.) This key is used to unlock the decryption key on each DVD. A DVD has 400 copies of the same unique decryption key, each encrypted with every unlock code. Note the global secret: if you manage to get one unlock key for one player, you can decrypt every DVD.

But even if this were all perfect, the scheme could never work.

The flaw in the security model. The software player eventually gets the decryption key, decrypts the DVD, and displays it on the screen. That decrypted DVD data is on the computer. It has to be; there's no other way to display it on the screen. No matter how good the encryption scheme is, the DVD data is available in plaintext to anyone who can write a computer program to take it.

And so is the decryption key. The computer has to decrypt the DVD. The decryption key has to be in the computer. So the decryption key is available, in the clear, to anyone who knows where to look. It's protected by an unlock key, but the reader has to unlock it.

M-14033

The DVD software manufacturers were supposed to disguise the decryption program, and possibly the playing program, using some sort of software obfuscation techniques. These techniques have never worked for very long; they only seem to force hackers to spend a couple of extra weeks figuring out how the software works. I've written about this previously in relation to software copy protection; you can't obfuscate software.

It might be a bitter pill for the entertainment industry to swallow, but software content protection does not work. It cannot work. You can distribute encrypted content, but in order for it to be read, viewed, or listened to, it must be turned into plaintext. If it must be turned into plaintext, the computer must have a copy of the key and the algorithm to turn it into plaintext. A clever enough hacker with good enough debugging tools will always be able to reverse-engineer the algorithm, get the key, or just capture the plaintext after decryption. And he or she can write a software program that allows others to do it automatically. This cannot be stopped.

If you assume secure hardware, the scheme works. (In fact, the industry wants to extend the system all the way to the monitor, and eventually do the decryption there.) The attack works because the hacker can run a debugger and other programming tools. If the decryption device and the viewing device (it must be both) is inside a tamperproof piece of hardware, the hacker is stuck. He can't reverse-engineer anything. But tamperproof hardware is largely a myth, so in reality this would just be another barrier that someone will eventually overcome. Digital content protection just doesn't work; ask anyone who tried software copy protection.

One more lesson and an observation.

The lesson: This is yet another example of an industry meeting in secret and designing a proprietary encryption algorithm and protocol that ends up being embarrassingly weak. I never understand why people don't use open, published, trusted encryption algorithms and protocols. They're always better.

The observation: The "solution" that the entertainment industry has been pushing for is to make reverse-engineering illegal. They managed in the United States: the Digital Millennium Copyright Act includes provisions to this effect, despite the protests of the scientific and civil rights communities. (Yes, you can go to jail for possessing a debugger.) They got a similar law passed inthe UK. They're working on the EU. This "solution" does not work and makes no sense.

First, unless reverse-engineering is illegal everywhere on the planet, someone will be able to do it somewhere. And one person is all you need; one person can write software that everyone else uses. Second, the reverse-engineer can -- like in this case -- work anonymously. Laws wouldn't have helped in this case. And third, laws can't put the cat back into the bag. Even if you could catch and prosecute the hackers who did this, it wouldn't affect the hacker tools that have already, and continue to be, written.

M-14034

What the entertainment industry can do, and what they have done in this case, is

use legal threats to slow the spread of these tools. So far the industry has threatened legal actions against people who have put these software tools on their Web sites. The result will be that these tools will exist on hacker Web sites, but will never be in public-domain software -- Linux, for example.

The fatal flaw is that the entertainment industry is lazy, and are attempting to find a technological solution to what is a legal problem. It is illegal to steal copyrights and trademarks, whether it is a DVD movie, a magazine image, a Ralph Lauren shirt or a Louis Vitton handbag. This legal protection still exists, and is still strong. For some reason the entertainment industry has decided that it has a legal right to the protection of its technology, and that makes no sense.

Moreover, they are badgering legislatures into passing laws that prop up this flawed technological protection. In the US and UK (and possibly soon in the EU), it is illegal to circumvent their technology, even when you never use it to violate a copyright. It is illegal to engage in scientific research about the encryption used in these systems. It is illegal to peek under the hood of this thing you have legally bought. So not only does this system not work, it creates a black market where there was none before, while doing no social good in the process.

This DVD break is a good thing. It served no ones interests for the entertainment industry to put their faith in a bad security system. It is good research, illustrating how bad the encryption algorithm is and how poorly thought out the security model is. What is learned here can be applied to making future systems stronger.

Bruce Schneier is the chief technology officer of Counterpane Internet Security Inc. and an author of one of the five encryption methods under consideration to become the United States' Advanced Encryption Standard.

M-14035

RealNetworks Wins Key Round Against Streambox

By TechWeb
Jan 19, 2000 (4:37 PM)
URL: http://www.techweb.com/wire/story/TWB20000119S0022

RealNetworks has won a preliminary injunction barring Streambox from distributing two products that RealNetworks says violate the federal Digital Millennium Copyright Act. RealNetworks had already won a temporary restraining order, which a U.S. District Court judge in Washington state this week turned into an injunction until the issue is resolved.

www.cmpnet.com
The Technology Network